



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/017,926	10/29/2001	Hiroshi Maruyama	JP920000300US1	1476

7590

09/15/2005

IBM CORPORATION  
INTELLECTUAL PROPERTY LAW DEPT.  
P.O. BOX 218  
YORKTOWN HEIGHTS, NY 10598

EXAMINER

SHIFERAW, ELENI A

ART UNIT

PAPER NUMBER

2136

DATE MAILED: 09/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/017,926

Applicant(s)

MARUYAMA ET AL.

Examiner

Eleni A. Shiferaw

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 22 June 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-29 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-29 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date: \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

ET

## DETAILED ACTION

### ***Response to Amendment***

1. Applicant's arguments/amendments with respect to amended claims 1, 7, 10, 11, 15, 16, 17, 18, 19, 20, added claim 29, and presently pending claims 1-29, filed on June 22, 2005 have been fully considered and are moot in new grounds of rejection. And also examiner does not agree with applicant's argument:

### ***Response to Arguments***

2. Applicant argues that:

a. The references, whether alone or in combination, fail to support independent claims 1, 7, 10, 11, 15, 16, 17, 18, 19, and 20 wherein *"the key for creating, or for verifying, a digital signature is selected based on the contents of the message document of the communication, wherein said contents of the message document of the communication, wherein said contents do not include any digital signature data"* (page 16, 17, and 18, par. 2, and page 19 and 20 par. 1).

However, Examiner disagrees with applicant.

Regarding argument (a), Argument is not persuasive. Godfrey teaches plurality of proxy servers that intercepts messages transmitted between application units and extracts the markup language data (form data) that is **not signed**, markup language data (form data) is an intercepted form filled with information that is sent from a user to be transmitted to

another user, and verifies and/or creates digital signature by determining what key to use to sign the received data based on the received **unsigned data** (col. 6 lines 66-col. 7 lines 13, and fig. 1). Moreover, applicant's arguments regarding claims 7 and 22 for not having argument (a) above is not persuasive because the argued limitation is not claimed on claims 7 and 22.

The examiner is not trying to teach the invention but is merely trying to interpret the claim language in its broadest and reasonable meaning. Therefore, the examiner asserts that the system of the prior art, references do teach or suggest the subject matter as recited in independent claims 1, 7, 10, 11, 15, 16, 17, 18, 19, and 20, All dependent claims are also rejected at least by virtue of their dependency on independent claims and by other reason set forth in this office action dated September 9, 2005. Accordingly, rejections are respectfully maintained.

3. Claims 1-29 are presented for examination.

***Claim Rejections - 35 USC § 102***

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1, 15, 17, 19, and 21 are rejected under 35 U.S.C. 102(e) as being anticipated by Liu et al. (Liu, Patent No.: US 6,760,752 B1).

As per claims 1, 17, 19 and 21, Liu teaches a proxy server/a storage medium means/a program transmission apparatus means for relaying communications between applications and for performing an additional process comprising:

storage for storing (col. 5 lines 60-col. 6 lines 10) a program that permits a computer to function as:

a key manager for managing multiple keys used to generate a digital signature to be provided for a message document that is exchanged between said applications (col. 2 lines 5-21; key manager manages plurality of public keys used to sign a signature); and

a signature key determiner for extracting said message document from a predetermined application, and for, based on said message document, determining a key used to provide a digital signature, wherein said contents do not include any digital signature data (Liu col. 19 lines 57-67; key manager extracts the packed data that is not signed and determines the signature key used to generate the signature by comparing the public key included as part of the packed data that is not signed with the public key recovered in the signature verification process); and

a signature generator for providing a digital signature for said message document by using said key that is obtained from said key manager based on a determination made by said signature key determiner, and for transmitting said message document with said digital signature to a destination application (col. 15 lines 24-31; based on the determination made by key server data is signed and transmitted to recipient).

As per claim 15, Liu discloses a computer-implemented digital signature method for providing a digital signature for a message document exchanged by applications and for authorizing said message document, comprising the steps of:

selecting, in accordance with the contents of a message document generated by one of said applications, a key used for providing a digital signature for said message document, wherein said contents do not include any digital signature data (Liu col. 19 lines 57-67; key manager extracts the packed data that is not signed and determines the signature key used to generate the signature by comparing the public key included as part of the packed data that is not signed with the public key recovered in the signature verification process);

providing a digital signature for said message document (col. 15 lines 24-31); and

transmitting said message document with said digital signature to a destination designated by said one of said applications (col. 15 lines 24-31; based on the determination made by key server data is signed and transmitted to recipient).

6. Claims 1-2, 5, 7, 15, 17, 19, 21-22, 25, and 27 are rejected under 35 U.S.C. 102(e) as being anticipated by Godfrey et al. (Godfrey, Patent No.: US 6,363,479 B1).

As per claim 1, 17, 19 and 21, Godfrey teaches a proxy server/a storage medium means/a program transmission apparatus means for relaying communications between applications (Godfrey Fig. 1 No. 108 & 110) and for performing an additional process comprising:

storage for storing (col. 2 lines 50-col. 3 lines 12) a program that permits a computer to function as:

a key manager for managing multiple keys used to generate a digital signature to be provided for a message document that is exchanged between said applications (Godfrey col. 6 lines 66-col. 7 lines 13; proxy 110 and 108 manage multiple keys to intercept messages exchanged between the application units 1, 2, & 3 and sign the intercepted messages with respective key); and

a signature key determiner for extracting said message document from a predetermined application, and for, based on said message document, determining a key used to provide a digital signature, wherein said contents do not include any digital signature data (Godfrey col. 7 lines 4-13; proxy 108 extracts the markup language data (form data) that is **not signed**, form data is an intercepted form filled with information that is sent from a user to be transmitted to another user, and determines what key to use to sign the received data based on the received **unsigned data**); and

a signature generator for providing a digital signature for said message document by using said key that is obtained from said key manager based on a determination made by said signature key determiner, (Godfrey Fig. 1 No. 120 & 118 and page 6 lines 66-page 7 lines 13; signature key is determined and message is signed by proxy), and for transmitting said message document with said digital signature to a destination application (Godfrey Fig. 1 No. 126; document is signed by proxy server and transmitted to the destination application or unit 1).

As per claims 7 and 22, Godfrey teaches a digital signature system/computer program product comprising:

applications for performing data processing (Godfrey col. 5 lines 50-51); and  
a proxy server connected to said applications via a network (Godfrey Fig. 1 No. 110, 108, 104, and 114),

wherein said proxy server intercepts a communication, transmitted through said network, from one of said applications to an external destination device, provides a digital signature for a message document exchanged via said communication based on the contents of said message document, wherein said contents do not include any digital signature data, and transmits said message document with said digital signature to said external destination device (Godfrey col. 7 lines 4-13, col. 4 lines 21-47 and Fig. 1 No. 104, 106, 118 and 120; proxy 108 extracts the markup language data (form data) that is **not signed**, form data is an intercepted form filled with information that is sent from a user to be transmitted to another user, and determines what key to use to sign the received data based on the received **unsigned data**).

As per claims 15, 25, and 27, Godfrey discloses a computer-implemented digital signature method/medium/program of instructions for providing a digital signature for a message document exchanged by applications and for authorizing said message document, comprising the steps of:

selecting, in accordance with the contents of a message document generated by one of said applications, a key used for providing a digital signature for said message document, wherein said contents do not include any digital signature data (Godfrey col. 7 lines 4-13; proxy



108 extracts the markup language data (form data) that is **not signed**, markup language data (form data) is an intercepted form filled with information that is sent from a user to be transmitted to another user, and selects what key to use to sign the received data based on the received **unsigned data**);

providing a digital signature for said message document (col. 6 lines 66-67); and  
transmitting said message document with said digital signature to a destination designated by said one of said applications (Godfrey Fig. 1 No. 126; document is signed by proxy server and transmitted to the destination application or unit 1).

As per claim 2, Godfrey discloses, the proxy server wherein said key manager sets multiple key selection rules for obtaining said key, and only when said key selection rules are satisfied can said signature generator obtain said key (col. 7 lines 4-13; only when the selected key is verified can said proxy generator obtains key and generates signature).

As per claim 5 Godfrey teaches the proxy server (Godfrey Fig. 1 No. 108 and 110), further comprising:

a log manager for storing said message document with a digital signature provided by said signature generator, and for managing a log (Godfrey Col. 5 lines 41-43).

7. Claims 7, 10-14 and 22-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Liu et al. (Liu, Patent No.: US 6,760,752 B1) in view of Gupta et al. (Gupta, Patent No.: US 6,658,565 B1).

As per claims 7 and 22, Liu teaches a digital signature system/computer program product comprising:

applications for performing data processing (Liu col. 2 lines 46-51); and  
server connected to said applications via a network (Liu fig. 108 and 102),  
server intercepts a communication, transmitted through said network, from one of said applications to an external destination device, provides a digital signature for a message document exchanged via said communication based on the contents of said message document, wherein said contents do not include any digital signature data, and transmits said message document with said digital signature to said external destination device (Liu col. 19 lines 57-67; key server obtains public key for verifying the message exchanged between sender and recipient based on the message not signed, and/or public key of not signed message received is verified with public key of signed signature).

Liu does not explicitly teach proxy server performing the verification;

However Gupta discloses intermediate stations, proxy or router, to verify digital signatures appended to frames and/or packets transmitted over the network (abstract).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Gupta within the system of Liu because they are analogues in digital signature verification (abstract). One would have been motivated to incorporate the teachings of proxy verifying a digital signature because it would route/transmits different confidential messages with in/out of a network.

As per claims 10 and 23, Liu teaches a digital signature verification system/computer program product comprising:

applications for performing data processing (fig. 2G); and

server intercepts a communication from an external destination device to an application transmitted through said network, obtains a public key for verifying a message document exchanged via said communication based on the content of the message document, wherein said contents do not include any digital signature data (Liu col. 19 lines 57-67; key server obtains public key for verifying the message exchanged between sender and recipient based on the message not signed, and/or public key of not signed message received is verified with public key of signed signature), verifies a digital signature provided for the message document exchanged via said communication using said public key to determine if the message document has been authorized (col. 19 lines 57-67; key server verifies the signature if it is from authorized person), and transmits said message document that has been authorized (col. 15 lines 24-31; key server signs the message and sends the message to recipient).

Liu does not explicitly teach proxy server performing the verification;

However Gupta discloses intermediate stations, proxy or router, to verify digital signatures appended to frames and/or packets transmitted over the network (abstract).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Gupta within the system of Liu because they are analogues in digital signature verification (abstract). One would have been motivated to incorporate the teachings of proxy verifying a digital signature because it would route/transmits different confidential messages with in/out of a network.

As per claims 11 and 24, Liu teaches a network system/computer program product comprising:

multiple groups connected to a wide area network, all of which have applications for performing data processing (fig. 1 and col. 1 lines 54-64);

server intercepts a communication transmitted by an application of a local group to an application of a different group, provides a digital signature for a message document exchanged via said communication based on the contents of said message document, wherein said contents do not include any digital signature data, and transmits said message document with said digital signature to said application of said different group (Liu col. 15 lines 24-31 and fig. 2A element 38 no. 2; key server provides digital signature based on the received message and transmits it to intended recipient), and

server intercepts a communication from said application of said different group to said application of said local group, selects a public key for verifying a message document exchanged via said communication, wherein said public key is selected based on the contents of the message document, wherein said contents do not include any digital signature data (Liu col. 19 lines 57-67; key server obtains public key for verifying the message exchanged between sender and recipient based on the message not signed, and/or public key of not signed message received is verified with public key of signed signature), verifies a digital signature provided for the message document exchanged via said communication using said public key to determine if the message document has been authorized (col. 19 lines 57-67; key server verifies the signature if it is from authorized person), and transmits said authorized message document to said application

of said local group (col. 15 lines 24-31; key server signs the message and sends the message to recipient).

Liu does not explicitly teach proxy server performing the verification;

However Gupta discloses intermediate stations, proxy or router, to verify digital signatures appended to frames and/or packets transmitted over the network (abstract).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Gupta within the system of Liu because they are analogues in digital signature verification (abstract). One would have been motivated to incorporate the teachings of proxy verifying a digital signature because it would route/transmits different confidential messages with in/out of a network.

As per claim 12, Liu and Gupta teach all the subject matter as described above. In addition, Liu teaches the network system, wherein, when said application of said local group transmits a message document, said proxy server stores the message document with a digital signature in a log, and manages said log (Liu fig. 1); wherein, when said application of said local group receives a message document from a different group (Liu col. 1 lines 66-col. 2 lines 4), said proxy server stores in a log a message document authenticated by a verification of a digital signature, and manages said log (Liu col. 1 lines 66-col. 2 lines 4, and col. 5 lines 60-col. 6 lines 9); and wherein, at a predetermined timing, the server compares the transmission log with the reception log for the same message document, and authorizes communication (Liu col. 5 lines 60-col. 6 lines 9).

As per claim 13, Liu and Gupta teach all the subject matter as described above. In addition, Liu teaches the network system, wherein said proxy server compares signature information for a digital signature concerning the same message document (Liu col. 19 lines 57-67).

As per claim 14, Liu and Gupta teach all the subject matter as described above. In addition, Liu teaches the network system, wherein said proxy server compares hash values used for providing a digital signature for the same message document (Liu col. 2 lines 5-10).

8. Claims 3-4, 6, 9, 16, 26, and 28-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Godfrey et al. (Godfrey, Patent No.: US 6,363,479 B1) in view of Spelman et al. (Spelman, Patent Number: 5,680,458).

As per claim 16, Godfrey teaches a digital signature verification method comprising: for verifying a digital signature provided for a message document exchanged by applications, and for authorizing said message document (Godfrey Col. 5 lines 37-41 and Fig. 1 No. 118, 120), including the steps of:

receiving a message document with a digital signature that used said original key (Godfrey Col. 5 lines 22-23);

Godfrey does not explicitly teach a providing and verifying digital signature in using a replacement key,

However Spelman discloses accepting a message document with a digital signature that uses a replacement key, when said digital signature on said received message document has been

provided by using said replacement key for an original key that is determined in accordance with the type of said message document (Spelman Col. 6 lines 47-63; the replacement public key that corresponds to the replacement private key and the digital signature that is generated using the central authority's replacement private key is verified and accepted along with the message);

Selecting a public key for verifying a digital signature, provided using said original key, said public key being selected based on the contents of the message document, wherein said contents do not include any digital signature data (Spelman col. 2 lines 34-38; appropriate public key is selected and used to verify digital signature based on electronic messages not signed); and

Verifying said digital signature provided using said original key to authorize said message document with said digital signature that uses said replacement key (Spelman Col. 6 lines 47-63 and col. 8 lines 65-col. 9 lines 6).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Spelman within the system of Godfrey because it would allow to effectively and efficiently provide the replacement key so that the public can trust a valid key (Spelman Col. 1 lines 52-57). One skilled in the art at the time of the invention was made would modify these teachings to receive a message document with a digital signature that used said original key after the message document signed using said replacement key has been accepted because it would additionally provide a digital signature that uses a private key.

As per claim 3, Godfrey and Spelman teach all the subject matter as described above. In addition, the proxy server (Godfrey Fig. 1 No. 108 and 110), wherein, when said key for

generating a digital signature for said message document can not be obtained, said signature generator employs a replacement key that is defined in advance to provide a digital signature (Spelman Col. 4 lines 65-col. 5 lines 8; when central authority's root key/private key has been compromised, the central authority selects a new replacement private/public key pairs, generated based on the root key/private key, and generates a digital signature using a replacement private key and sends the generated digital signature along with the replacement public key to the user).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Spelman within the system of Godfrey because it would allow to effectively and efficiently provide the replacement key so that the public can trust a valid key (Spelman Col. 1 lines 52-57). One skilled in the art at the time of the invention was made would modify these teachings and use a replacement key when a key selection rules set for said key are not established or satisfied because it would provide digital signature when key selection rules are not established.

As per claim 4, Godfrey and Spelman teach all the subject matter as described above. In addition, the proxy server, wherein, after said signature generator has provided a digital signature using said replacement key (Spelman Col. 4 lines 65-col. 5 lines 8), when said acquisition condition that is determined for the original key based on said message document is satisfied to enable the acquisition of said original key (Spelman Fig. 1 No. 16 and 18), said signature generator again provides a digital signature using said original key (Godfrey col. 6 lines 66-col. 7 lines 3; proxy 110 and 108 provide signatures again to enhance security).



As per claim 6, Godfrey and Spelman teach all the subject matter as described above. In addition, the proxy server, wherein said log manager stores not only said message document for which said signature generator has provided a digital signature using said replacement key (Spelman Col. 3 lines 22-27), but also said message document without digital signature; and wherein said signature generator obtains, from said log manager, said message document without said digital signature, and provides a digital signature using said original key (Godfrey Fig. 1 No. 112, 114, and 120). The rationale for combining are the same as claim 15 above.

As per claim 9, Godfrey and Spelman teach all the subject matter as described above. In addition, the digital signature system, said proxy server employs a predetermined replacement key to provide a digital signature (Spelman Col. 4 lines 65-col. 5 lines 8); and wherein, when said key selection rules for said key are satisfied after said digital signature has been provided using said replacement key (Spelman Col. 4 lines 65-col. 5 lines 8), said proxy server again employs said key to provide a digital signature for said message document (Godfrey col. 6 lines 66-col. 7 lines 3; proxy 110 and 108 provide signatures again to enhance security).

As per claim 26, both Godfrey and Spelman teach all the subject matter as described above. In addition, Godfrey teaches an article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing a digital signature verification method, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 16 (Godfrey Col. 3 lines 60-63).

As per claim 28, both Godfrey and Spelman teach all the subject matter as described above. In addition, Godfrey program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for a digital signature verification method, said method steps comprising the steps of claim 16 (Godfrey Col. 3 lines 60-63).

As per claim 29, Godfrey teaches all the subject matter as described above. Godfrey discloses wherein key selection rules are provided for said key and further comprising the steps of:

providing a digital signature for said message document (fig. 1 element 118);

using said key, when said key selection rules for said key have been satisfied, to again provide a digital signature (page 6 lines 66-page 7 lines 3; proxy 110 and 108 are again generating digital signature to enhance security); and

transmitting said message document with said digital signature to said destination (fig. 1 element 126).

Godfrey fails to explicitly teach wherein providing signature for the message document, when key selection rules set for said key are not established, by using a replacement key that is set in advance for said key;

However Spelman discloses generating a digital signature using replacement key (Spelman Col. 4 lines 65-col. 5 lines 8; when central authority's root key/private key has been compromised, the central authority selects a new replacement private/public key pairs, generated based on the root key/private key, and generates a digital signature using a replacement private

key and sends the generated digital signature along with the replacement public key to the user);

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Spelman within the system of Godfrey because it would allow to effectively and efficiently provide the replacement key so that the public can trust a valid key (Spelman Col. 1 lines 52-57). One skilled in the art at the time of the invention was made would modify these teachings and use a replacement key when a key selection rules set for said key are not established or satisfied because it would provide digital signature when key selection rules are not established.

9. Claims 18 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boeyen et al. (Boeyen, Patent No.: US 6,675,296 B1) in view of Spelman et al. (Spelman, Patent Number: 5,680,458).

As per claim 18, Boeyen teaches a storage medium on which input means of a computer stores a computer-readable program that permits said computer to perform:

a process for selecting a key used to provide a digital signature for a message document in accordance with the contents of message document transmitted from a predetermined application, wherein said contents do not include any digital signature data (Boeyen Fig. 6, Fig. 7 and page 6 lines 67-col. 7 lines 6; certificate generator selects and use appropriate key to generate digital signature based on the received data/format ID that does not include digital signature);

a process for providing said digital signature for said message document using said key that is selected (Boeyen Fig. 7 No. 700, 26, and 32), when key selection rules for said key used to provide a digital signature for said message document have not been satisfied (Boeyen Fig. 6 and Fig. 7; when signature format, 212a or 212b is selected, the selector selects the appropriate private key based on the data has been received and applies digital signature based on the rule. For example: if 212a is selected use first signature private key else if 212b is selected use second signature private key); and

a process for employing said key to provide again a digital signature for said message document, when said key selection rules for said key are satisfied after said digital signature has been provided using said replacement key (Boeyen Col. 2 lines 66-col. 3 lines 1, fig. 6 No. 212a or 212b and col. 6 lines 62-col. 7 lines 18; to generate a second digital signature using an appropriate key when signature format is selected).

Boeyen does not explicitly teach employing a predetermined replacement key to provide said digital signature for said message document;

However Spelman discloses generating a digital signature using a predetermined replacement key (Spelman Col. 4 lines 65-col. 5 lines 8; when central authority's root key/private key has been compromised, the central authority selects a new replacement private/public key pairs and generates a digital signature using a replacement private key and sends the generated digital signature along with the replacement public key to the user);

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Spelman within the system of Boeyen

because it would allow to effectively and efficiently provide the replacement key so that the public can trust a valid key (Spelman Col. 1 lines 52-57).

As to claim 20, it has similar limitations as claim 18; therefore, it is being rejected under the same rationale over Boeyen and Spelman. In addition, Boeyen teaches:

transmission means for reading said program from said storage means, and for transmitting said program (Boeyen Fig. 1 and col. 5 lines 13-49).

10. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Godfrey et al. (Godfrey, Patent No.: US 6,363,479 B1) in view of Owen (Patent Number: 5,483,595).

As per claim 8, Godfrey discloses wherein said proxy server permits a key used to provide a digital signature to be verified in accordance with the contents of a message document; and wherein said proxy server sets key selection rules for said key and permits digital signature using said key when said key selection rules have been satisfied (col. 7 lines 4-13; when the selected key is satisfied/verified proxy permits digital signature).

Godfrey fails to teach keys to be changed.

Owen discloses different sized keys that have different security level and when a user wants higher security, user selects the longest key to provide security, and when less security required small sized key is selected (col. 4 lines 4-23 and fig. 1 element 50).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to select different keys. One skilled in the art would have been motivated to do so because it would provide higher security for highly secure digital data (col. 4 lines 4-23)

### *Conclusion*

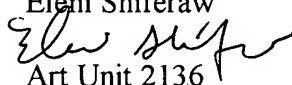
11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).


A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Eleni Shiferaw  
  
Art Unit 2136  
September 9, 2005

  
Primary Examiner  
AU 2131  
9/12/05